Section 2.7

Mechanical Systems

Contents

Contents

Item	Page Number

TABLES

FIGURES

Section 2.7
Mechanical Systems

2.7.1. Personnel Access Control Systems and Shield Doors

2.7.1.1. Purpose

The purpose of equipment shield doors on caves is to allow the main maintenance equipment, e.g., cranes and power manipulators, out of the main cave to a point where man access can be allowed. The personnel access control system is a system of robust interlocks and access doors that allow safe access to the equipment for maintenance.

2.7.1.2. Description

The shield door in a cave consists of large steel plates plus other material if required to provide the shielding when in a closed position. They operate by hydraulic or electric drives. To open, some will slide; others swing to produce an opening which allows a crane and or power manipulator to pass through. In highly active caves, there will be two sets of doors and in-between there will be decontamination facilities which will allow the crane or power manipulator to pass through the second doors to a maintenance area where operators will be able to work.

The access system is controlled through hard-wired logic linked to radiation monitors and mechanical locks preventing the opening of personnel access doors into the maintenance areas. It will also prevent locking-in any operators with the use of slave keys, burst out locks, summon assistance, and emergency stop buttons.

In extreme situations, the cave inventory may need to be moved for access to the decontamination so that the radioactivity behind the first door is acceptable. This is interlocked with the monitors in that area.

Figure 2.7-1 shows typical access and door arrangements.

2.7.1.3. Hazardous Situations

During normal operations, men will not routinely be in these maintenance areas, but when they are, the hazards are increased exposure to radiation. Depending on the layout and thickness of the cave walls, there could be an increase in radiation at the end wall if both doors are allowed to be open simultaneously.

2.7.1.4. Outline of Procedure for Personnel Entry into Maintenance Area

Below is outlined a typical arrangement for personnel entry into a maintenance area associated with a cave. This demonstrates the defense in depth arrangements to prevent radiation hazard to personnel entering such an area. There are numerous facilities on the Sellafield site that utilize such a system and while details may differ, the principles remain the same.
Hazards other than radiation exposure, such as contamination and industrial hazards (e.g., moving machinery), will be controlled by a safe system of work which will identify the personal protective

equipment required. Depending on specific application, other equipment may be incorporated into the interlock system.

2.7.1.4.1. Entry into the Maintenance Area

A person of authority (manager) has to justify a need to go into the maintenance area. He will ensure that a safe system of work is in place for the task that is required.

As defense in depth, the manager would carry out various pre-checks prior to allowing entry. (For example, visual checks through windows to ensure that cave doors are closed and that gamma monitors are showing anticipated readings.)

This person will then use his “management key” to release the “door master key” at the control station. This key release is interlocked to the gamma monitors in the maintenance area and shield doors. High gamma readings or open shield doors will prevent the “door master key” from being released.

Once the “door master key” is removed, the interlock prevents opening of the shield doors.

Each person entering the maintenance area would sign the safe system of work log after being briefed on the task requirements and safety arrangements. They would also reassure themselves that the shield doors are closed through visual inspection through windows.

The door master key would then be inserted into the door lock key exchange. Each person going into the maintenance area would take a slave key from the key exchange. The door master key cannot be removed until all slave keys have been returned.

If larger numbers of personnel need to enter the maintenance area together, then a lock-out box system can be utilized to maintain integrity of the system.

Personnel entering the maintenance area would wear personal alarm dosimeters with preagreed alarm levels. They would be briefed to immediately vacate the maintenance area if the action level is reached or if area gamma monitors alarm.

Prior to entry, they would also check that the door warning signs are not in alarm (alarms linked to gamma monitors in maintenance areas).

The Personnel Access Door can now be carefully opened. Radiation levels would be measured at the point of entry to confirm the gamma monitor readings.

Personnel can now enter the maintenance area.

During entry, the Personnel Access Door would be closed. The door would have some form of “burst-out” mechanism to prevent personnel being trapped in a cave.

The first task upon entry would typically be to do a detailed radiation survey of the work area, to be fed back into the safe system of work.

In the maintenance area there are Summon Assistance buttons, and emergency stop buttons in event of problems with moving machinery. A “tally person” in the entrance area can then summon further assistance.

2.7.1.4.2. Exit From Maintenance Area

After completion of the work in the maintenance area, personnel would put their slave key back into the Door Lock Key Exchange. They would then also sign the safe system of work form. Only after all of the slave keys have been returned can the door master key be released to lock the door.

The manager would confirm that everybody had signed off the safe system of work. Only then would he use the Door Master Key to release the management key. He would then sign the safe system of work form to confirm all work in the maintenance area is completed and that normal plant operations could then resume.

This will then remove the interlocks to allow operation of shield doors.

The set of important safety SSCs for the above hazardous situations (or faults) is provided in the following table. The table also identifies the Safety function and the Design Safety Features.

Figure 2.7-1. Cave Crane, Access, and Door Arrangements

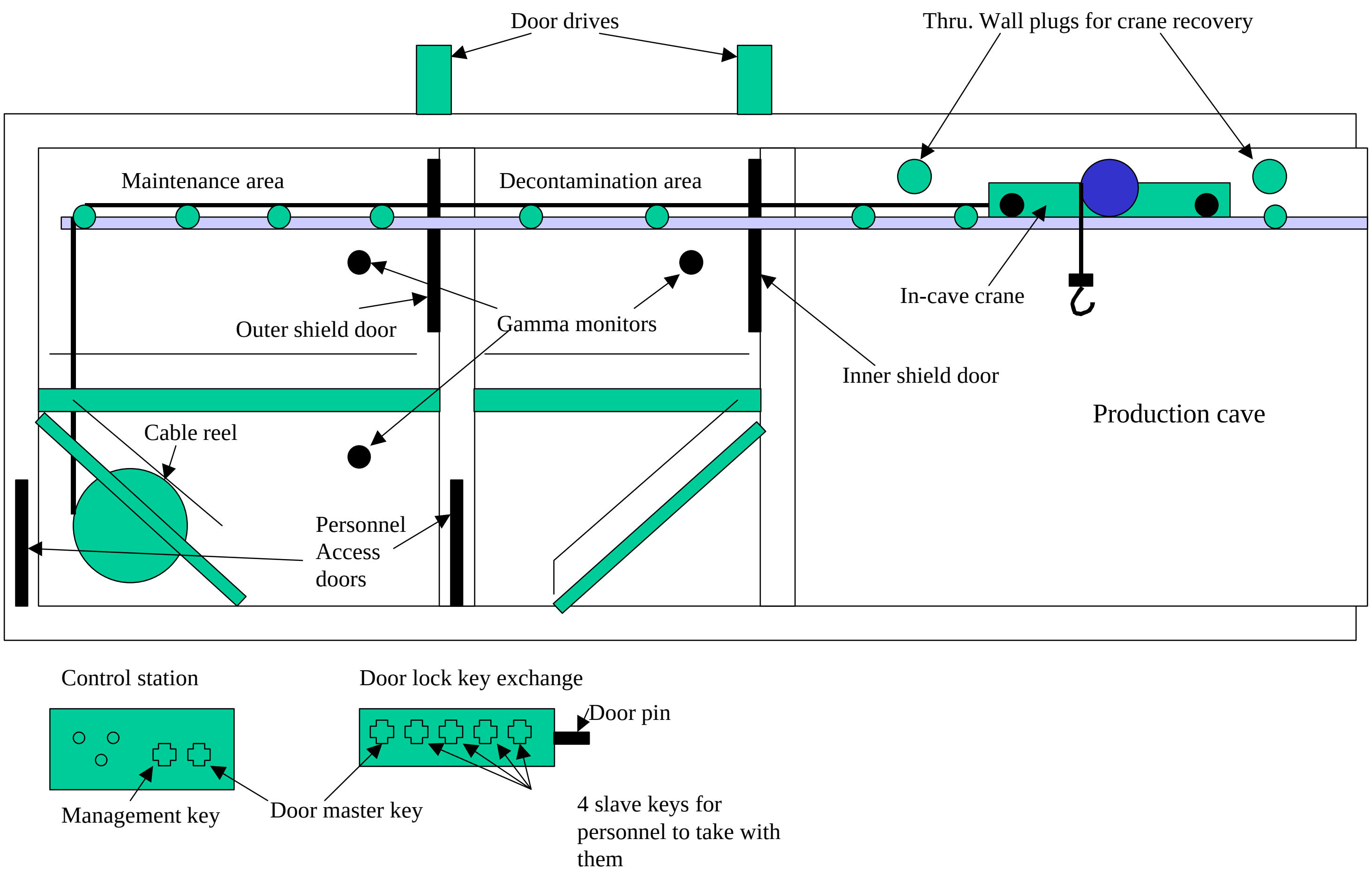

Table 2.7-1. Personnel Access Control Systems and Shield Doors

Fault	Important to Safety SSCs	Safety Function	Design Safety Feature
High personnel exposure on entry, during occupancy, or due to personnel being locked in the area after resumed operations.	Personnel access control system (i.e., Monitoring) Shield doors and personal access (PA) doors Interlocks between shield and personnel access doors and a key exchange system.	To prevent access during high radiation To prevent exposure To track individuals	The doors are passive when closed. Administrative controls are used to initiate access, by releasing the management key. This is then backed up by the access system, which uses radiation monitors linked to hard-wired isolation with the master key. (as required other equipment that could move sources or represent a conventional hazard will be interlocked as well)Followed by key exchange for individual tracking, which then allows access. The PA doors will have burst-out latch designs and Emergency stop/ assistance buttons will be located in the area. All active interlocks will fail safe on loss of power.
High personnel exposure due to doors opening together.	Interlock system	To allow only one door at a time to be open.	Hard-wired interlocks on door drive and positions. Only required if walls around maintenance areas can not be thick enough or operators need to be in the maintenance area when equipment or sources are being transferred. All active interlocks will fail safe on loss of power.

2.7.2. Cave Cranes

2.7.2.1. Purpose

To lift and move product and production equipment around the in cave areas for production and maintenance needs.

2.7.2.2. Description

In-cave cranes that are used for production and maintenance work have been developed over many years to provide a reliable and effective way of lifting and moving in-cave loads. They have all the features of normal cranes and are normally rail bridge with cross-bogie type cranes, but other layouts have been used (i.e., polar). In addition to some of the standard features being rated, a significant proportion of the crane is of modular design. This is done to aid and speed up maintenance of what could be a contaminated system. The cranes are usually controlled from fixed control stations and interlocked to allow only one station to have control at any one time. The stations will be located at cave windows and be supported by CCTV.

The recovery from motive failure in a remote cave location (e.g., motor failure or loss of power) is a main consideration in the design of in-cave cranes. The system typically consists of through-wall plugs to allow tool engagement with the hoist drive to allow lowering of any load. The main down cave cable is provided with tension elements to allow hauling of the crane back to the maintenance facility.

A diagram of a cave crane is shown in Figure 2.7-2.

2.7.2.3. Hazardous Situations

In normal operation, the main safety functions which an in-cave crane and moving loads must perform are:

- Not to drop the load, i.e., no free fall of the load.
- Not to run the load or crane into other equipment.

Either of these could lead to a release of activity which may challenge the confinement systems (cave and ventilation).

The set of important SSCs for the above hazardous situations (or faults) is provided in the following table. The table also identifies the Safety function and the Design Safety Features.

Figure 2.7-2. Cave Crane

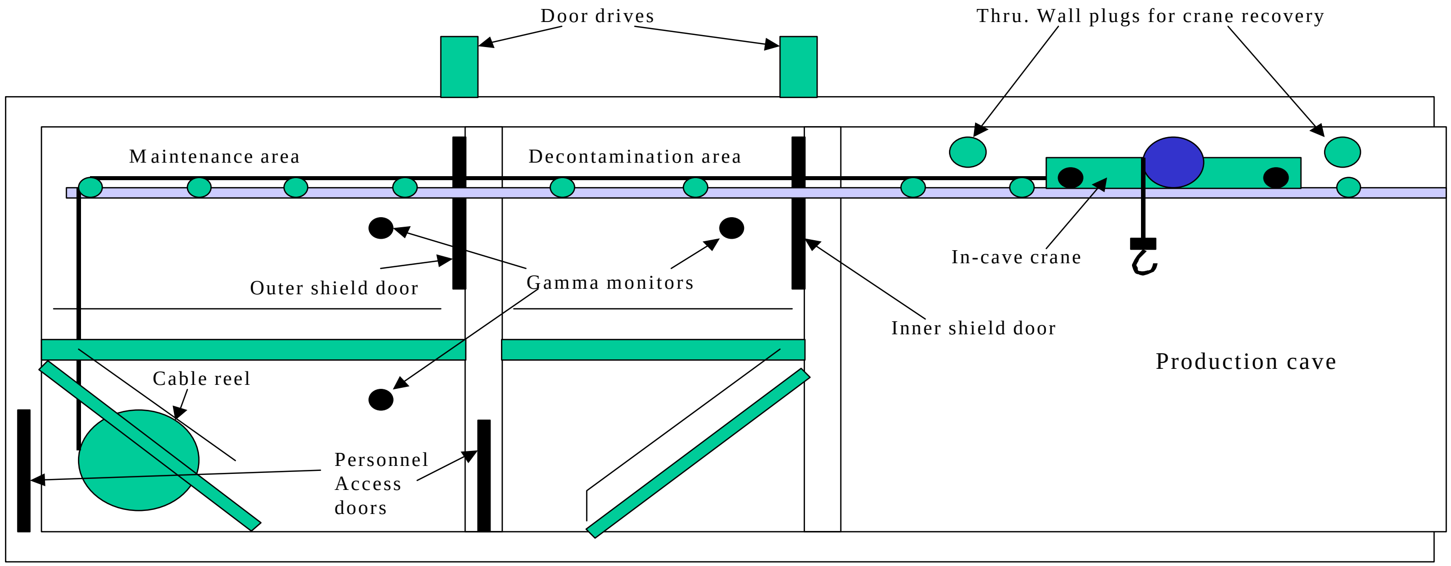

Table 2.7-2. In-Cave Cranes

Fault	Important to Safety SSCs	Safety Function	Design Safety Feature
Load drop leading to a challenge to cave and ventilation confinement systems	Vertical load path (crane design).	To support the maximum load. To withstand the seismic event if required.	The passive strength of all load path components, and if required, seismic qualification.
	Crane active systems. (List in DSFs)	To hold load on power failure. To hold load in any motor or control fire to prevent rope mechanical damage or overstressing, or hoist failure leading to load drop.	Based upon the severity of drop not all cranes may have these features, all active features will be fail safe on loss of power. Crane active systems (This list is based on the BNFL in cave crane current practices) Hoist Protection Devices: Hoist operating limits Unit (Speed Control Service and back-up Brakes (2 off brakes) Brake Calipers (quantity as required Hoist ultimate over raise Slack rope protection Overload protection General Crane Safety/Protection Features: Hard-wired Emergency Stop System Operator Control Stations Defense in depth: The cave ventilation systems provide mitigation if a release is the result of any damage.

Table 2.7-2. In-Cave Cranes

Fault	Important to Safety SSCs	Safety Function	Design Safety Feature
Horizontal impact of crane and or load with other equipment during normal load handling (e.g., shield doors) leading to a challenge to the confinement systems.	Rail layout (or crane coverage), zone crane moves, and interlocks with doors.	Limit crane coverage, limit crane coverage, and prevent impact.	Passive (design review of equipment and rail layout). With the following active systems. Cross Traverse Protection Devices: Traverse Normal Operating Limits Long Travel Protection Devices: Travel Normal Operating Limits Use positional switches or encoders to interlock equipment areas. Impact buffers are also provided. Defense in depth: The cave ventilation systems provide mitigation if a release is the result of any damage.

2.7.3. In-Cave Trolley

2.7.3.1. Purpose

To move active product, e.g., containers, in a horizontal direction between work stations.

2.7.3.2. Description

This is a mechanical system consisting of a set of rails along which a 4-wheeled trolley/bogie can run. Located alongside a shield-wall and, in most cases, the shielding on the other sides forms a tunnel around the trolley and rails. At the end of the tunnel or facility will be a system of shield doors through which the rails and a cable pass. The motive force is provided by one axial being electrically powered. The electrical power is provided by the cable, which is pulled out of a reeling system, as the trolley moves away from the reel and the reeling system pulls the cable back in when the trolley moves toward the reel. The reeling system is located behind the shield doors. The trolley may have other functions at the various workstations but these functions will be activated buy through wall drives at the station and be arranged to fail safe or be recoverable.

The recovery from motive failure in a remote tunnel/cave location (e.g., motor failure or loss of power) is a main consideration in the design of in-cave trolleys (see Figure 2.7-3). The system typically consists of a main down tunnel/cave cable being provided with tension elements to allow hauling of the trolley back to the maintenance facility.

2.7.3.3. Hazardous Situations

In normal operation the container handling system has limited safety functions, only that of positioning the load correctly and not running into the shield doors.

The set of important SSCs for the above hazardous situations (or faults) is provided in the following table. The table also identifies the Safety function and the Design Safety Features.

Figure 2.7-3. In-Cave Trolley

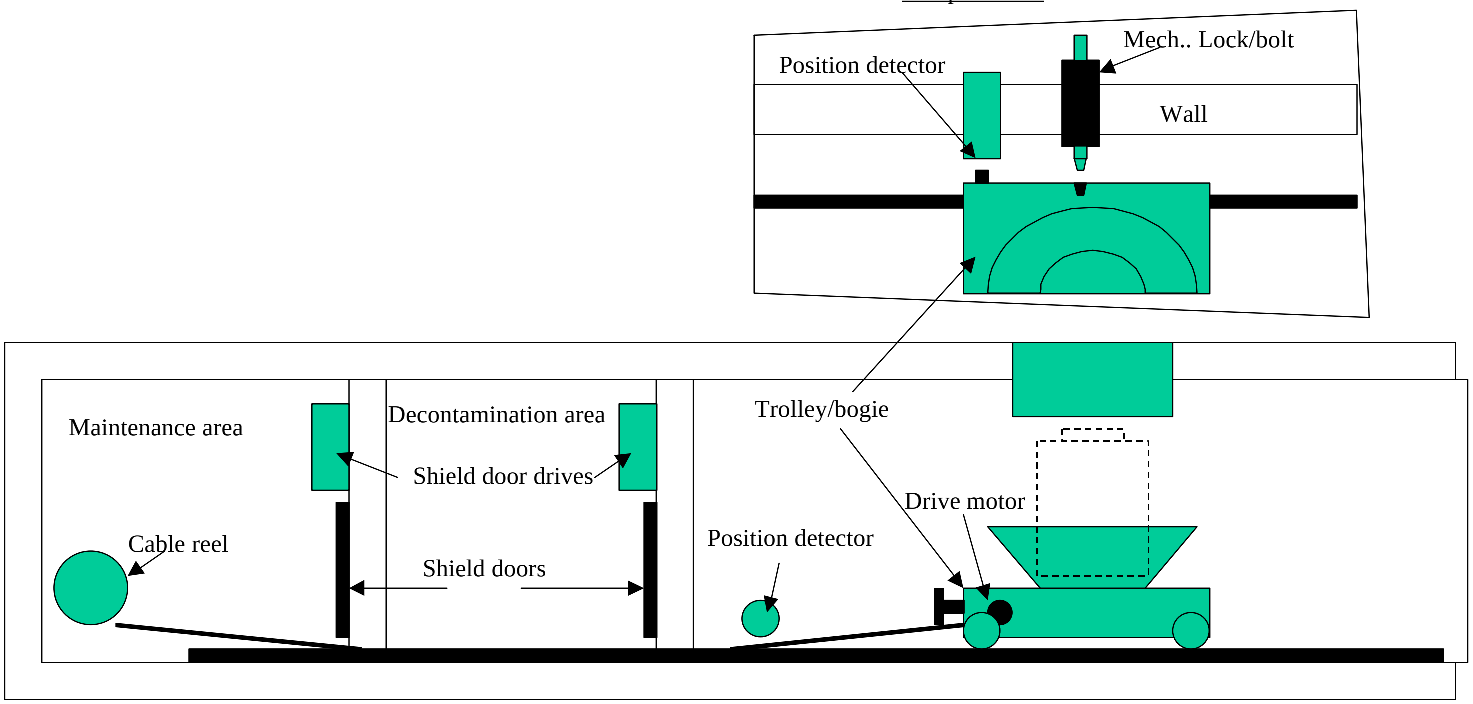

Table 2.7-3. In-Cave Trolley

Fault	Important to Safety SSCs	Safety Function	Design Safety Feature
Mis-positioning (e.g., at the container fill station so giving rise to a glass spill in the tunnel/cave) resulting in a challenge to the ventilation systems.	Position interlock (usually large mechanical lock bolt)	Accurate alignment	If possible will usually be mechanical (e.g., if the container fill station is considered, the air supply for the melter discharge system will have an isolation valve linked to the trolley lock/bolt). Active interlocks will fail safe on loss of power. For Defense in Depth The normal control system will contain the same logic and be driven from positional switches. The cave and ventilation systems provide mitigation if a spill occurs.
Horizontal impact with shield doors or other equipment.	Over travel limit switches or proximity sensors	Prevent impact	Active interlocks will fail safe on loss of power. For Defense in Depth The normal control system will contain the same logic and be driven from separate positional switches Also the mechanical design will assume impact and in most cases this will result in the fitting of shock absorbers.

2.7.4. Out-of-Cell Cranes

2.7.4.1. Purpose

Out-of-cell/cave cranes are used for the lifting and moving of equipment or product. If the items are contaminated or active, they will be inside a cask/flask. (Note: The majority of cranes will be used for non-active or non-routine maintenance and will consist of simple monorail systems.)

2.7.4.2. Description

(Note this description is to aid DSF understanding, so the simple maintenance cranes are not referred to again.)

Out-of-cell/cave cranes that are used for production and maintenance work, lifting active loads are usually high integrity cranes. The specifications for high integrity cranes have been developed over many years to provide a reliable and effective way of lifting and moving active loads. They have all the features of normal cranes and are normally rail bridge with cross-bogie type cranes but other layouts have been used; i.e., underslung. In addition to some of the standard features being rated, a number of extra features are added to improve the reliability of the load supporting function (see the list in the following table). The cranes are usually controlled from fixed control stations and interlocked to allow only one station to have control at any one time.

2.7.4.3. Hazardous Situations

In normal operation, the main safety function which a high integrity crane moving active loads must perform are:

- Not to drop the load, i.e., no free fall of the load.
- Not to run the load into other equipment.

Either of these could lead to a release of activity that may challenge the confinement systems (cave and ventilation) or damage other SSCs.

The set of important SSCs for the above hazardous situations (or faults) is provided in the following table. The table also identifies the Safety function and the Design Safety Features.

Table 2.7-4. Out-of-Cell Cranes

Fault	Important to Safety SSCs	Safety Function	Design Safety Feature
Load drop resulting in the release of activity	Vertical load path (crane design)	Not to drop load To withstand the design basis seismic event without load drop.	The passive strength of all load path components including seismic qualifications.
	Crane active systems. (List in DSFs)	To hold load on power failure. To hold load in any power or control fire. To prevent rope mechanical damage or overstressing, or hoist failure leading to load drop.	Based upon the severity of drop not all cranes may have these features: (all active features will fail safe on loss of power) Crane active systems (This list is based on the BNFL high integrity crane) Hoist Protection Devices: Hoist operating limits Eddy Current Brake (ECB) Unit (Speed Control Service and back-up Thruster Brakes (2 off identical brakes) Emergency Rope Barrel Brake Calipers (quantity as required Hoist ultimate over raise Slack rope protection Overload protection Over speed protection General Crane Safety/Protection Features: Hard-wired Emergency Stop System Operator Control Stations

Table 2.7-4. Out-of-Cell Cranes

Fault	Important to Safety SSCs	Safety Function	Design Safety Feature
Horizontal impact with other equipment during normal load handling leading to release of activity.	Rail layout Active interlocks	Limit load path Inhibit crane movement	Passive (design review of equipment and rail layout). Active systems: (all active features will fail safe on loss of power) Cross Traverse Protection Devices: Traverse Normal Operating Limits Over Traverse Ultimate Limit Long Travel Protection Devices Travel Normal Operating Limits Over Travel Ultimate Limit Functional testing of hard wired interlocks
Horizontal impact with other equipment during non-routine maintenance.	Procedures and training	Prevent impact	Specific job hazards review and operational oversight.
Lifting flask too high resulting in release of activity if dropped.	Limited lift height	Prevent flask from being lifted above analyzed safe height	Passive design of crane lifting beam and flask.

2.7.5. Mobile Gamma Gates and Bottom Entry Flasks

2.7.5.1. Purpose

To move active product or equipment outside and between the main caves and cells.

2.7.5.2. Description

This is a mechanical system consisting of a gamma gate and bottom entry flask. A gamma gate is a shielded transfer port permitting the breach in containment for transferring radioactive material or equipment between a shielded flask and a shield cave or cells, as is a door that can only be opened when a flask is present. In the case of mobile gamma gate, the complete gate can be removed but only if a shield plug has been placed in the hole into the cell or cave. The bottom entry flask is a shielded and sealed container with a door on the bottom face, which can be opened only when the flask is placed on a gamma gate. There is a hoist-on and a grapple in the flask for lifting the item to be moved.

A high integrity overhead crane normally moves the flask.

A diagram of a gamma gate and flask is shown in Figure 2.7-4.

2.7.5.3. Hazardous Situations

In normal operation the gamma gate and flask must maintain containment and shielding. The hazards are therefore incorrect operation resulting in a loss of shielding or containment and dropping the flask. The possible fouling of the internal hoist with the doors or in cave/cell equipment may challenge the shielding and containment so they noted on the table.

The set of important SSCs for the above hazardous situations (or faults) is provided in the following table. The table also identifies the Safety function and the Design Safety Features.

Figure 2.7-4. Gamma Gate and Flask

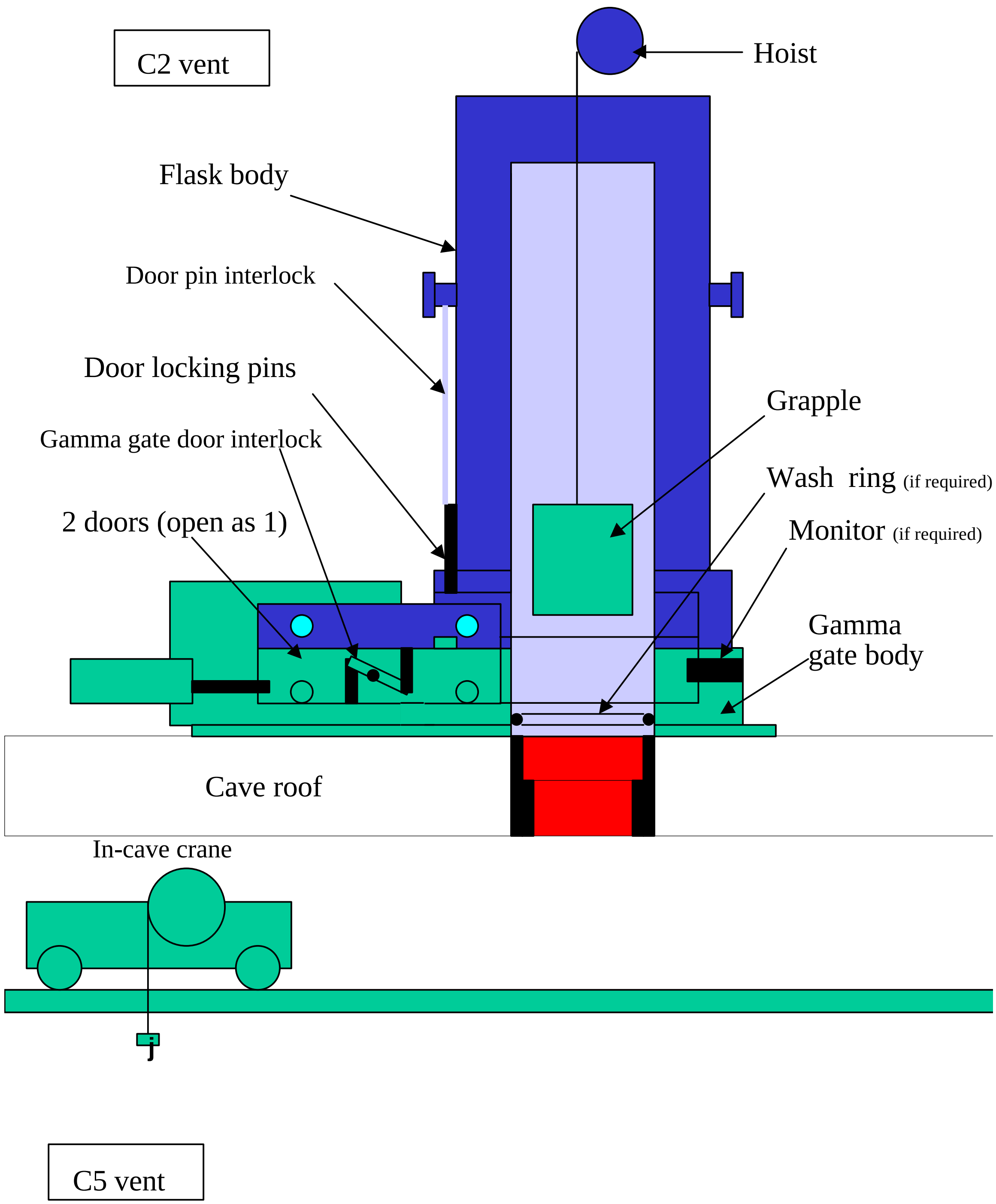

Table 2.7-5. Mobile Gamma Gates and Bottom Entry Flasks

Fault	Important to Safety SSCs	Safety Function	Design Safety Feature
Lift flask off gamma gate with doors open (loss of shielding)	Interlock system, which allows the flask to be removed only when doors are closed and locked.	Doors must be closed before flask is removed.	This is achieved with robust mechanical and backed up electrical interlocks that prevent the fitting of the lifting beam if the doors are not closed and locked. The incorporation of both mechanical and electrical interlocks provide protection from common mode, common cause failure. All active interlocks are fail safe on loss of power. Defense in depth: The normal control system will contain the same logic.
Gamma gate door opened with no flask in place. (loss of shielding)	Interlock system which only allows the doors to open with a flask in place.	Doors can only open when flask is in place.	A mechanical lock is activated by the weight of the flask and along with electric interlocks associated with the “plugging in” of the flask power and control cable. The incorporation of both mechanical and electrical interlocks provide protection from common mode, common cause failure. All active interlocks are fail safe on loss of power. Defense in depth: The normal control system will contain the same logic.
Flask hoist fails to fully raise, load fouls doors (manual recovery required)	Interlock with fully raised switch and door drive.	Door will not close (or open)	Hard-wired interlocks that only allow doors to move if hoist is fully raised. All active interlocks are fail safe on loss of power. Defense in depth: The normal control system will contain the same logic.
Flask hoist operation foul in cave equipment movements (damage to equipment)	Interlock with fully raised switch and equipment drives or hoist drive and equipment position.	Only operate hoist if other equipment is not moving or is in a safe location	Hard-wired interlocks that only allow the hoist to operate only if other equipment is safe or the hoist move inhibits the equipment movement. All active interlocks are fail safe on loss of power.

Table 2.7-5. Mobile Gamma Gates and Bottom Entry Flasks

Fault	Important to Safety SSCs	Safety Function	Design Safety Feature
			Defense in depth The normal control system will contain the same logic.
Gamma gate removed with no plug in place (loss of shielding)	Interlock with plug fitted and the gamma gate lifting trunnion.	Gamma gate can only be removed with plug fitted.	Hard-wired interlocks that only clears lifting trunnion on gamma gate when plug is detected in position. All active interlocks are fail safe on loss of power. Defense in depth: The normal control system will contain the same logic.
Drop of flask resulting in release of activity.	Flask body including shield door	Provide containment and shielding post drop.	The flask will be qualified to maintain containment and shielding if dropped from a defined maximum height. Flask must therefore be protected from being lifted above this height. The qualification will also take account of the drop of the internal load and any chemical/corrosion systems that may challenge the integrity of the flask.
Dropped loads (In-flask hoist failure)	In-flask overload testing facility Equipment restraints and supporting features, in-cell, in breakdown cave and the maintenance workshop	To check condition of the in-flask hoisting mechanisms To prevent loss of confinement as a direct result of a dropped load from the flask	Flask testing is a scheduled maintenance policy. Facilities are provided to perform safe maintenance. Equipment supports are designed and configured to prevent secondary structural damage to the fabric of the confinement system

2.7.6. Power Manipulators

2.7.6.1. Purpose

To lift, move and work on maintenance equipment in the main production caves.

2.7.6.2. Description

In-cave power manipulators that are used for maintenance work have been developed over many years to provide a reliable and effective way of lifting, moving, and working on in-cave equipment. They are normally rail bridge with cross-bogie mounting. The bridge and cross-bogie are very similar to the in-cave crane and are of modular design. This is done to aid and speed up maintenance of what could be a contaminated system. The power manipulator is system of links and joints mounted on the end of a telescopic master (if required) that is hung from the cross-bogie. On the end of the links and joints is usually a wrist with a jaw assembly but other tools can be fitted and powered. The power manipulator is usually electrical and controlled from fixed or plug in control stations and interlocked to allow only one station to have control at any one time. The stations will be located at cave windows and be supported by CCTV.

The recovery from motive failure in a remote cave location (e.g., motor failure or loss of power) is a main consideration in the design of in-cave manipulators (see Figure 2.7-5). The system typically consists of through-wall plugs to allow tool engagement with the manipulator drive if required to allow freeing of any load. The main down-cave cable is provided with tension elements to allow hauling of the power manipulator back to maintenance facility.

2.7.6.3. Hazardous Situations

In-cave power manipulators are not involved in normal operation so the only safety function is not to run into or miss use the power manipulator on other equipment. Which could result in the failure of primary confinement.

The set of important SSCs for the above hazardous situations (or faults) is provided in the following tables. The table also identifies the Safety function and the Design Safety Features.

Figure 2.7-5. Power Manipulator

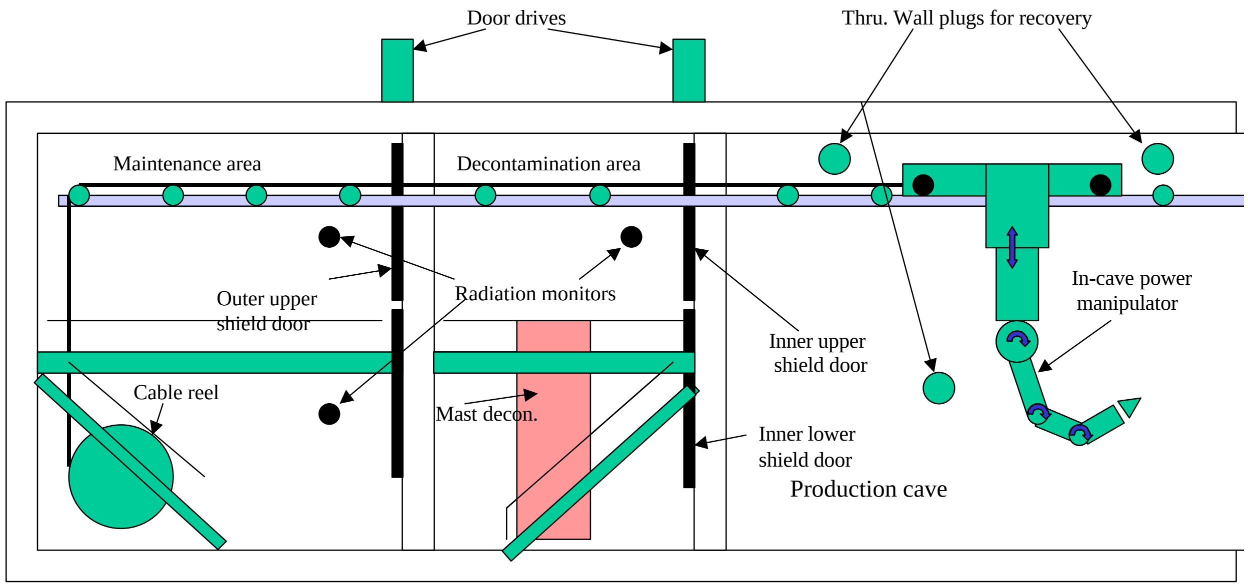

Table 2.7-6. Power Manipulators

Fault	**Important to Safety SSCs**	**Safety Function**	**Design Safety Feature**
Horizontal impact of power manipulator with other equipment during operations (e.g. shield doors) resulting in a release of activity that could challenge the ventilation systems.	Rail layout (or power manipulator coverage) Zone power manipulator moves. Interlocks with doors	Limit path Prevent impact	Passive (design review of equipment and rail layout). Active systems (all active features will fail safe on loss of power) Cross Traverse Protection Devices: • Traverse Normal Operating Limits • Over Traverse Ultimate Limit Long Travel Protection Devices: • Travel Normal Operating Limits • Over Travel Ultimate Limit Interlock design For Defense in Depth The cave and ventilation systems provide mitigation if a leak occurs.
Misuse of the power manipulator on other equipment (which can not be interlocked or zone out) resulting in a release of activity that could challenge the ventilation systems.	Training and design simple maintenance tasks	To prevent damage to other equipment.	The design of the other equipment always takes account of the “power” of the manipulators. Training is provided in the use of the manipulator and the individual tasks are designed to be as simple as possible. Tasks are initially perform during inactive testing and fully recorded for future training and records. For Defense in Depth: The cave and ventilation systems provide mitigation if a leak occurs.